International Journal of Advanced Engineering Research and Science (IJAERS)
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-8, Issue-2; Feb, 2021
Journal Home Page Available: https://ijaers.com/
Journal DOI: 10.22161/ijaers
Article DOI: https://dx.doi.org/10.22161/ijaers.82.1

A Literature Review about Smart Contracts Technology

David Nadler Prata[1], Humberto Xavier de Araújo[2], Cleórbete Santos[3]

[1,3]Department of Computer Science, Federal University of Tocantins, Palmas -TO, Brazil
[2]Department of Electrical Engineering, Federal University of Tocantins, Palmas-TO, Brazil

Received: 15 Nov 2020;

Received in revised form:

17 Jan 2021;

Accepted: 25 Jan 2021;

Available online: 06 Feb 2021

***Keywords*— blockchain, smart, contracts, criptocurrency, internet**

Abstract*— This work begins with an explanation of fundamental concepts about Bitcoin and Blockchain and then explores the main definitions of smart contracts in the updated literature, demonstrates some categories of smart contracts, explores the most widely used platforms that support smart contracts, and gives greater prominence to the Ethereum platform for its more robust characteristics regarding the creation and storage of this type of contract. It then concludes by demonstrating the advantages of smart contracts in relation to traditional contracts, as well as addressing their legal validity.

I. INTRODUCTION

It was at the beginning of 2009 that a person or group of people named Satoshi Nakamoto released Bitcoin, a peer-to-peer solution that allows the transfer of values and payments by unconventional means [1]. This technology was primarily restricted to the universe of system programmers, but over the years it has gained popularity and attracted the attention of diverse institutions such as banks, governments, among others [2]. Currently, the basic technology for Bitcoin, Blockchain, considered disruptive, has several utilities, among them data storage, digital asset transfer and transaction management, through a decentralized computer architecture. Another technology that has emerged in the blockchain field is intelligent contracts, or smart contracts, which work by automating contractual clauses through triggers created in software. These triggers previously created and configured can be, for example, specific dates, where certain terms of a contract will be executed.

II. BITCON AND BLOCKCHAIN

In 2008, Satoshi Nakamoto, possibly a pseudonym under which one or more people remain anonymous, expressed the need to create a more secure and reliable payment system, using proof of trust based on cryptography, and dispensing with the use of third parties, such as banking institutions, for its operation, is to say, a transfer of values could be made directly between those interested, without the need for an intermediary [1]. Launched in 2009, the Bitcoin open source technology allows value transfers to occur through the use of bitcoin cryptocurrency, generated by the system itself, with a public blockchain managing and storing transactions, and aiming at reducing fees, such as those applied by banks, and facilitating negotiations at the international level. Bitcoin was the first decentralized cryptocurrency to be created and the nodes connected to its blockchain use a proof-of-work based consensus algorithm, formed by rules that define how the blocks containing the transactions will be added to the existing blockchain. These nodes, which are computational devices participating in the Bitcoin network, that is, the public blockchain that maintains it, need to solve a computational challenge to have the right to add a new transaction block to the current blockchain, being rewarded with bitcoins when they do so, in a process called cryptocurrency mining [3]. Another aspect of the public blockchain used for the storage of bitcoin transactions is the immutability of their data, which ensures the legitimacy of all the information stored on the network, provides a history of operations performed and allows their auditability and traceability. In addition, Bitcoin is decentralized, allowing its users to make the validations of all transactions made, that is, the entire network can check how many bitcoins the user accounts have received or sent through a mechanism of consensus among all participants that guarantees the legitimacy of the operations [4].

III. SMART CONTRACTS

Blockchains are structures that allow several functionalities, being Bitcoin the most famous example. Due to their versatility, besides transactions involving values expressed in cryptocurrencies, these networks allow data storage, decentralized real estate registration, order tracking, among other applications, such as smart contracts, the main focus of this work. In the computing world, any assets of the physical world can have their characteristics, such as price, color, weight, owner, etc, expressed by means of software, also including the so-called intangible assets, such as rights, personal data, certificates, trademarks, among others. Blockchains serve for this purpose of safe and reliable storage of such digital assets, as well as propitiate that the relations between these assets can occur by means of computer programming, that is to say, by means of smart contracts, which serve to execute, in an automated manner, certain commands based on preestablished instructions and conditions. However, despite having the term "contract" in their title, smart contracts are not considered contracts in the legal sphere, serving only as an instrument for the execution of clauses present in the contracts themselves [5].

The term smart contracts was coined by Nick Szabo in 1994. This researcher defined smart contracts as computerized transaction protocols that execute contract terms [6]. For other authors, smart contracts are software originally designed to use the reliable computational features of a blockchain network in order to automatically implement conditions that two parties can agree to when they sign a contract in an untrusted environment [7]. Another definition is that smart contracts are computer programs that can be executed in a network of mutually trusted nodes, such as the blockchain, without the intermediation of a trusted authority, and that, due to their resistance to manipulation, such "smart contracts" are useful in several scenarios, especially in those that require money transfers in respect of certain rules agreed by those involved, such as in financial services [3]. Smart contracts are also considered as digital contracts that allow the creation of clauses dependent on a decentralized consensus that are tamper-proof, and are typically self-applicable through automated execution, but without the legal nature of traditional contracts and without using artificial intelligence resources [8]. In a concept closer to computing, smart contracts are, in short, small programs that aim to automate tasks based on conditional "if" and "then" instructions, stored and executed without intermediaries in a decentralized manner in several devices connected in a peer-to-peer network, capable of fulfilling contractual clauses [9]. Still under the context of computing, smart contracts are software that implements a logical sequence of steps according to certain clauses and rules, and consist, conceptually, of three parts: the computational code that represents the contract logic; the set of messages that the smart contract can receive and that represents the events that will activate the contract; and the set of functions that will activate the reactions foreseen by the contract logic [7].

About to the types of smart contracts, there are some categories mentioned in the literature, such as financial smart contracts, which aim at transactions involving monetary values. Some of these contracts certify the ownership of an asset of the physical world, its value, and serve to monitor negotiations involving such assets. Others, also of this financial strain, are created for collective financing (crowdfunding), receiving values from investors who have an interest in helping certain projects financially. Another use for these smart contracts has been the creation of high-yield investment programs based on Ponzi (pyramid) schemes, which receive money from interested parties with the promise of a return with interest on the amount invested as other interested parties join the project. Some of these contracts provide insurance in the face of digitally verifiable setbacks, such as a delay of a particular flight at an airport, triggering a refund transfer operation for the beneficiary. Other notarial smart contracts take advantage of the immutability of data present in blockchains to register ownership of assets and guarantee their origin. Some of these are used for document hash storage, ensuring the existence and integrity of these assets. This type of smart contract is also used for the protection of copyrights in music, art and photography files, among others, as well as to associate users public keys to their real identity. There are also smart contracts of the digital wallet category, aimed at managing cryptographic keys, sending transactions, serving as intermediaries in interaction with blockchains. Finally, there is the library category, composed of smart contracts that have functions that are implemented by other smart contracts. These functions can be for value conversion, text conversion, etc [3].

Smart contracts can be created and maintained in several available blockchain implementations. Bitcoin, as already commented, is a solution that aims primarily at the transfer of values by means of bitcoin cryptocurrency, in a decentralized manner, using a public blockchain that registers all the transactions that have occurred. Bitcoin's infrastructure allows the use of a scripting language with limited resources, however its open model and data immutability have guided the development of other protocols that allow the creation of basic versions of smart contracts. Another platform that also works in its own blockchain and has a consensus algorithm similar to that of Bitcoin is Ethereum, whose cryptocurrency is called Ether (ETH). Ethereum allows the development of smart contracts through programming languages such as Solidity. The contracts are triggered through transactions sent to Ethereum's blockchain and the effects are validated by the network. In the Ethereum universe both users and smart contracts can send and receive cryptocurrencies ether among themselves. The Stellar platform, which also has its own blockchain, uses a consensus algorithm based on the Byzantine Agreement Protocol [10], which provides lower resource consumption to validate blocks of data in relation to the cryptographic puzzle required by Bitcoin in its validation and mining operations. Unlike Ethereum, Stellar does not have its own language for the creation of smart contracts, but allows contracts of this type to be made using the transactions that occur in its network. Besides those mentioned above, there is Lisk, which also has its own cryptocurrency and allows the creation of private blockchains, where their owners can define access privileges for third parties. In Lisk smart contracts can be made in Javascript or Node.js language and work on separate blockchains, although transactions using the contracts can be made involving the main blockchain of the platform [3].

Blockchains that support smart contracts are also called "programmable blockchains" [11], and Ethereum, among the platforms listed, has the most smart contracts in its blockchain [3]. Ethereum allows both the storage and execution of smart contracts, and because of the inherent characteristics of blockchains, it is possible to trace the operations of these contracts. As mentioned, in this platform smart contracts are written in Solidity language, which is similar to Javascript, and the structure of the code is in the format of a class, Object Oriented Programming (POO) concept. Like the Java compiler, Solidity produces bytecodes from the source code of the smarts contracts, and these bytecodes, after being stored in the blockchain of the platform, can be executed through the Ethereum Virtual Machine (EVM). To facilitate the coding of smart contracts, Solidity allows the creation of libraries and subcontracts. Subcontracts allow developers to establish object-oriented relationships between smart contracts, through, for example, inheritance and interfaces. Libraries provide code reuse and serve to encapsulate utility functions such as conversions and mathematical operations. When ready to go into production, smart contracts can be deployed on the network through a transaction sent to Ethereum's blockchain, also called a "contract creation transaction". After their deployment, smart contracts receive an address in the blockchain, and through this address it will be possible to send transactions to access the functions present in these contracts [11].

With regard to the advantages of smart contracts over traditional contracts, risk reduction can be cited: due to the immutability of blockchains, smart contracts cannot be arbitrarily changed once they are issued. In addition, all transactions that are stored and executed on all distributed blockchain systems are traceable and auditable. As a result, malicious behavior such as financial fraud can be greatly mitigated; Reduced administrative and service costs: blockchains ensure the reliability of the entire system through consensus mechanisms distributed among participating devices without passing through a central intermediary or mediator, and smart contracts stored on these networks can be automatically triggered in a decentralized manner. Because of this, administration and maintenance costs can be significantly reduced; Increased efficiency of business processes: the elimination of dependence on intermediaries can significantly improve the efficiency of business processes. For example, in a blockchain used for supply chain tracking, financial settlement can occur automatically between the participants of the peer-to-peer network, once the pre-defined conditions in smart contracts are met, significantly reducing the return time of transactions [4].

In the literature, there is still no consensus whether smart contracts can have the same legal validity as traditional contracts [12], although some authors consider that this type of agreement is a form of tutelage that exempts the intervention of the Judiciary for its execution, because regardless of the subsequent will of the parties, the terms will be executed when certain conditions are reached [13]. In the legal system of several nations, contracts are instruments that create, modify or extinguish legal relations between two or more contracting parties, and transactions carried out in this context by means of smart contracts have legal effects such as those derived from classic contracts. Another requirement that must be present in smart contracts for their legal effectiveness is the expression of the parties expression of will, which must be free and without vices. Smart contracts also have a fiduciary character, i.e. they are guarantors that the agreement will be fulfilled. In addition, they differ from traditional contracts by their purely digital nature, although they may serve to execute operations involving non-digital assets, such as real estate, immaterial rights, etc. Another peculiarity of this more modern version of the contracts is that they are fully implemented in software and have a double nature in legal terms: the smart contract code will be considered an intellectual property right at the same time as the contract will be considered a legally valid document as to what has been agreed between the parties involved. Furthermore, smart contracts increase the certainty of execution of the contractual clauses, are of a software-encumbered nature, are self-enforcing and self-sufficient, in the latter case, in that they do not require registration with intermediaries [13].

IV. CONCLUSION

As seen, the technology of smart contracts is not new, having been coined still in 2008, but it came to have greater dissemination and adhesion when establishing blockchains, like the one available on the Ethereum platform, the most used today for this type of digital agreement, although other solutions, such as the famous Bitcoin also allow its use, within certain limitations. Smart contracts, in their most basic definition, are representations in software of terms of a contract, which is executed through conditional operations present in computational algorithms. Some categories of smart contracts are listed in the literature, which take into consideration their purpose, such as financial, notarial, portfolio and library smart contracts, respectively, those aimed at value transfer operations, those for the registration of assets and immaterial rights, those that manage operations involving blockchain addresses and those that serve to create utility functions reusable by other smart contracts. In legal terms, smart contracts can be used for the creation, modification or termination of legal relationships, they are similar to traditional contracts in that they represent the expression of the will of the contracting parties, and differ from them in that they are purely digital in nature, they are fully implemented in software, and they are dual in nature in that their source code is an intellectual property right and the contract is a legally valid document. In addition, they increase the degree of certainty of their execution, ensure their result by means of software, are self-executable and self-sufficient, dispensing, in this case, with their prior registration.

REFERENCES

[1] NAKAMOTO, Satoshi. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[2] European Central Bank. (2015). Virtual currency schemes - a further analysis.

[3] BARTOLETTI, Massimo; POMPIANU, Livio. (2017). An empirical analysis of smart contracts: platforms, applications, and design patterns.

[4] ZHENG, Zibin et al. (2019). An overview on smart contracts: Challenges, advances and platforms.

[5] PERUGINI, Maria L; DAL CHECCO, Paolo. (2015). Smart Contracts: A Preliminary Evaluation.

[6] SZABO, Nick. (1996). Smart Contracts.

[7] PINNA, Andrea et al. (2019). A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics.

[8] CONG, Lin William; HE, Zhiguo. (2019). Blockchain Disruption and Smart Contracts.

[9] GRAAF, TJ de. (2019). From old to new: From internet to smart contracts and from people to smart contracts.

[10] MAZIÈRES, David. (2014). The Stellar consensus protocol: A Federated Model for Internet-level Consensus.

[11] OLIVA, Gustavo A; HASSAN, Ahmed E; JIANG, Zhen Ming. (2020). An exploratory study of smart contracts in the Ethereum blockchain platform.

[12] SAVELYEV, Alexander. (2017). Contract law 2.0: ‘Smart’ contracts as the beginning of the end of classic contract law.

[13] RASKIN, Max. (2017). The Law and Legality of Smart Contracts.